SIM-Based WLAN Authentication for Open Platforms

Ameen Ahmad
Business Development/Initiative Manager
Emerging Platforms Lab
Intel Corporation

Roger Chandler
Market Development Manager
Emerging Platforms Lab
Intel Corporation

Abhay A. Dharmadhikari
Senior Software Engineer
Emerging Platforms Lab
Intel Corporation

Uttam Sengupta
Principal Engineer, Staff Architect
Emerging Platforms Lab
Intel Corporation

Table of Contents

(Click on page number to jump to sections)

SIM-Based WLAN Authentication for Open Platforms

Ameen Ahmad
Business Development/Initiative Manager
Emerging Platforms Lab
Intel Corporation

Roger Chandler
Market Development Manager
Emerging Platforms Lab
Intel Corporation

Abhay A. Dharmadhikari
Senior Software Engineer
Emerging Platforms Lab
Intel Corporation

Uttam Sengupta
Principal Engineer, Staff Architect
Emerging Platforms Lab
Intel Corporation

Overview: Extending SIM Authentication to WLAN

Worldwide, traditional cellular operators are investigating how to integrate wireless local area networks (WLANs) into their service offerings and business models. Currently, GSM (global system for mobile communications) operators provide subscriber identity modules (SIMs) for each subscriber on their network. The role of SIM is to authenticate the user on the GSM network and to facilitate effective billing.

Operators are now seeking to extend this SIM-authentication functionality to WLAN services, instead of the existing username/password or prepaid service WLAN authentication methods. This article provides a brief overview of the authentication process in a GSM network, and then describes a possible method of WLAN authentication using SIM cards. It also goes through various SIM security issues, and describes an assortment of reader attachments and their advantages and disadvantages.

SIM in GSM Networks

The role of SIM in GSM networks is to ensure that only authorized users can access the network. In order to properly authenticate a user, a network must be able to store data, guard against unauthorized access to the stored data, and execute a cryptographic algorithm under secure conditions. The SIM and mobile device is authenticated with a background system. The data transferred between the mobile station and base station across the air interface is encrypted.

As shown in **Figure 1**, there are three major components in the GSM network:

- The mobile station (or mobile phone) that has the subscriber identity module (SIM), which provides the user's unique identity.
- The base station subsystem (BSS), which connects the user on a mobile station to other mobile/landline users.
- The network subsystem (NSS), which is capable of routing calls from fixed networks via the base station controllers (BSCs) and base transceiver stations (BTSs) to different mobile stations.

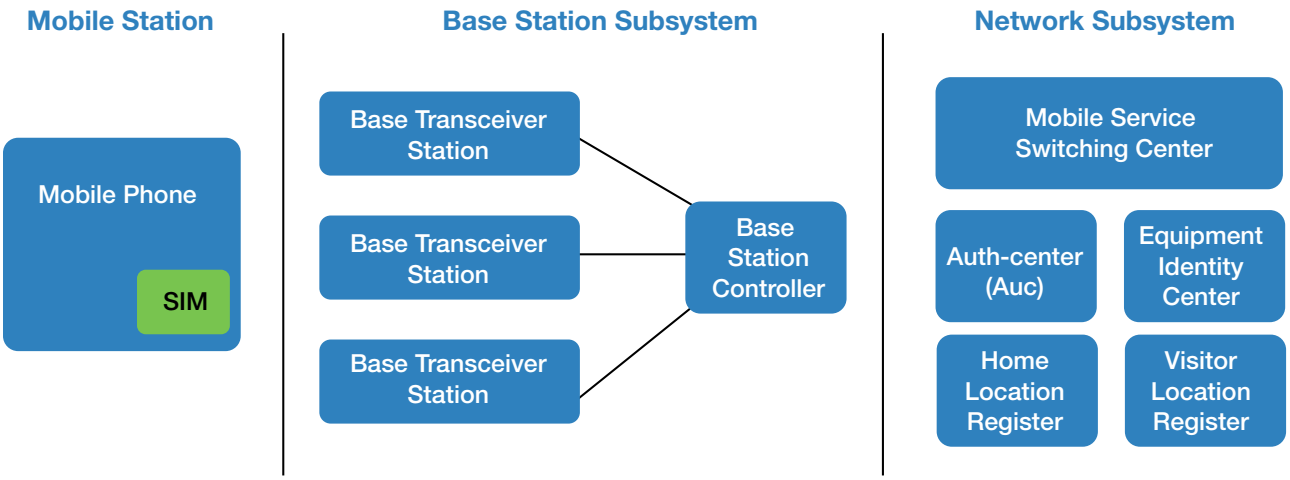

Figure 1. GSM network

The SIM authentication procedure on GSM networks checks the validity of the subscriber's SIM card and then decides whether the mobile station is allowed on a particular network. The parties involved in the authentication process are: a) the end user or holder of the SIM card, a non-grey listed (not stolen) and certified handset and b) the network operator (GSM service provider).

The authentication process is one-way since the user is being first authenticated to the phone via the PIN number and then to the operator via their SIM AAA (authentication, authorization, and accounting services) mechanism. The network authenticates the subscriber through the use of a challenge-response method:

1. When a subscriber wants to conduct conversation, the mobile station sets up a link to the base station and relays the IMSI (international mobile subscriber identity) or TMSI (temporary mobile subscriber identity) from the SIM to the base station.
2. If the subscriber's IMSI registers at the base station, the mobile station receives the 128-bit random number (RAND) transmitted through air interface, which is passed to SIM.
3. The RAND is passed to the SIM card, which is sent through A3 algorithm together with key (Ki). The output of A3 algorithm is the signed response (SRES).
4. The result is a cipher text block, SRES, which is transferred from the mobile station to the base station via the air interface.
5. The network subsystem, which is linked to the base station, derives the card-specific key from IMSI and performs computation similar to the SIM and generates SRESes.
6. The SRES sent to the network subsystem is then compared with the SRESes to authenticate the subscriber and thus authorize him/her to place a call.
7. Background system and SIM use A8 algorithm with RAND number and card-specific key (Ki) to compute the temporary ciphering key (Kc), which is used to encrypt data for transmission through the air interface.
8. The computed key (Kc) is then passed from SIM to mobile station, which performs data encryption and decryption using A5 algorithm.

Value of SIM-Based Authentication

Authentication allows an operator to ensure that only legitimate subscribers in the possession of an operator-supplied SIM card (using a handset that is not stolen) are the only ones allowed to make calls on the network. Authentication ensures that the network is being used by a paying customer and the call ends up generating actual revenue for the operator.

There are some inherent weaknesses in the GSM security system and algorithms that make it vulnerable to fraud. Two types of fraud are possible:

- Making “free” calls using a stolen SIM and/or equipment
- Making “free” calls using a cloned SIM

The European Telecommunications Standards Institute (ETSI), the GSM standards body, has been making several improvements in GSM security (improved cryptographic algorithm, etc.), while GSM operators have set up a sophisticated fraud detection and management system. For example, GSM networks prohibit duplicate SIMs to be active simultaneously, GSM handsets will not work without a SIM, and handsets are verified against a database to determine if they are stolen and are then restricted to emergency calls only.

SIM-Based Authentication for WLAN Networks

SIM-based WLAN authentication requires the use of a SIM reader attached to the computing device (**Figure 2**) so that the authentication software can use the SIM credentials.

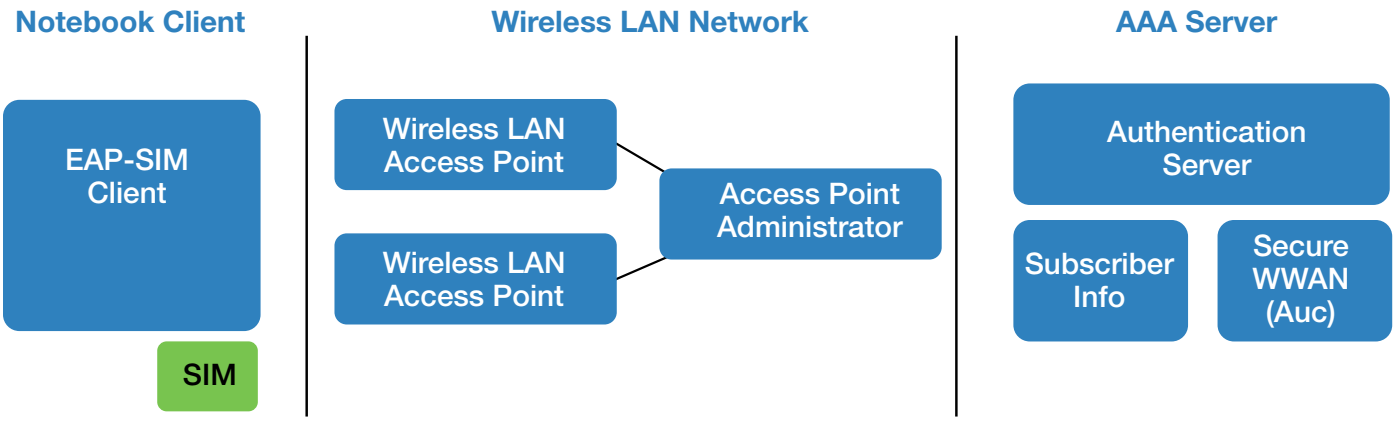

Figure 2. WLAN network

The EAP-SIM protocol, resident on the client, specifies the extensible authentication protocol (EAP) mechanism for authentication and session key distribution using GSM SIM. In EAP-SIM, a number of RAND challenges are used for generating several 64-bit ciphering keys (Kc), which are combined to constitute a longer session key.

EAP-SIM also enhances the basic GSM authentication mechanism by accompanying the RAND challenges with message authentication code in order to provide mutual authentication. The EAP-SIM client starts the authentication process by connecting to the AAA server. The AAA server issues a challenge over the 802.11b radio interface, which is then forwarded to the SIM reader by the EAP-SIM client. The EAP-SIM client communicates to the SIM through the SIM reader, the SIM calculates the response that contains the SRES and Kc, which is then sent to the EAP-SIM client. The EAP-SIM client forwards the response to the AAA server, which then checks the response and provides access appropriately. In this scenario it is assumed that the AAA server has a secure connection to GSM-backbone network components like home location register (HLR).

Use of SIM Cards on Open Platforms

An open platform, for the purposes of this article, is defined as a general-purpose computing device with an open operating system. A notebook PC is considered to be an open platform since users can download/write software for execution in a notebook PC without any restrictions.

There are various types of SIM readers available as an external attachment to personal computers as described below:

USB/PCMCIA SIM Access: This is currently the most common way to access a SIM card. In this usage model, a USB (universal serial bus) SIM reader and SIM reader driver software can be purchased or provided by an operator for use on a notebook computer. The USB SIM reader is a PC/SC standard compliant reader so it is accessible using the Microsoft* smart card subsystem. The USB SIM card reader is treated as a generic smart card reader. The smart card access is provided using a generic set of API from Microsoft* Resource Manager. The application can use the GSM 11.11 specification and Microsoft API for interacting with SIM cards. The USB readers are very easy to use and there are no additional regulatory requirements for using them to access SIM. However, the user has to physically remove the SIM from the cell phone and insert it into the USB reader. In general, physical access to a SIM in a cell phone is not easy. Another issue with USB readers is that the data path to and from the SIM is over an open bus and is thus susceptible to SIM attacks.

SIM Access from GPRS PC Cards: PCMCIA (Personal Computer Memory Card International Association) cards provide GPRS (general packet radio service) network access for notebook computers. PCMCIA GPRS cards and access software are provided by GPRS service providers. The GPRS card contains a GPRS radio, a slot for the SIM, and the firmware software. GPRS cards are installed as modems on notebook computers. Accessing SIM from a GPRS card for use in WLAN authentication is a very flexible and easy usage model. The biggest advantage is that the user already has a subscription for GPRS service. Also, the SIM is always present in the GPRS card so there is no need for the user to physically take out the SIM card from another device, such as a cell phone, and place it in a GPRS card. As is the case with USB readers, there is no need to satisfy any additional regulatory requirements. However, the data path used by the application/authentication software to access the SIM over the AT modem interface is still not completely secure.

*SIM Access from Mobile Handset over Bluetooth**: In this usage scenario the notebook connects to the handset over a Bluetooth connection. The notebook has a SIM access client, which connects to the SIM access server on the handset. The SIM access server is preinstalled on the phone/handset. The request for SIM data is passed from the notebook to the SIM access server on the phone. The data between the links is encrypted using Bluetooth baseband encryption. There are many steps involved in this, and not all phones currently support the required SIM access subsystems. This approach reuses the SIM on the cell phone SIM and the user does not have a SIM reader attached to the notebook. The phone acts as a remote SIM reader connected over a Bluetooth connection. This usage scenario doesn't cover the potential hacking of the authentication software, and it has open system issues similar to those associated with the USB or GPRS card reader.

SIM Access from Reader Hardwired to Notebook: This method modifies the current notebook architecture and provides the SIM reader with a secure access to the device; for example, not over current open USB or PCI buses. This is not a very flexible approach, since the legacy systems will not be able to support these modifications. This method may also require full type approval (FTA). At present, FTA is required for WWAN (wireless wide area network) modules with integrated SIM. This architecture will require modifications to the existing WWAN module, thus requiring new FTA. This approach provides complete data path security.

SIM Security for WLAN Authentication

SIM cards are a subset of smart cards—actually, SIM is an application on a smart card. In general, smart card security is guaranteed by four components:

- Card body
- Chip hardware
- Operating system
- Application

The chip hardware, operating system and application protects the data and programs in the smart card micro controller. Also, in the GSM system, SIM is manufactured, provisioned, distributed, and managed in trusted environments. This results in the SIM being a tamper-resistant device in which the access credentials of a mobile network subscriber can be securely stored. However, even if the key data (Ki) inside the SIM cannot be directly obtained, its opacity depends on the algorithms used to hide it from the outside world.

Using cryptanalysis, hackers can find a way to calculate the value of the secret data by analyzing a huge number of command response pairs. The risks of such attacks in cellular systems are, however, relatively low since the cell phone is "closed" to the outside world and also depends on the weakness of the cryptographic algorithm used (for example, Comp 128-1).

One possibility open to hackers is to eavesdrop on the data being transmitted between the cell phone and the base station. This approach requires having access to the cellular infrastructure, such as base station stations, for capturing the triplets (RAND, SRES, Kc) while they are transmitted over the air. Since the infrastructure equipment is quite expensive, this approach is not quite realistic.

Another approach is for the hacker to have physical possession of a stolen or cloned SIM. For this reason, operators use software to detect the usage of cloned SIMs and block them without impacting customer service. Also, GSM systems have fraud detection mechanisms in place to deter usage of stolen or cloned SIMs.

Open Platform Security

The use of SIM cards for authentication of users with open platforms in WLAN networks requires consideration of the openness of data paths used to access the SIM data (see **Figure 3**). Possible open paths are Path A and Path B.

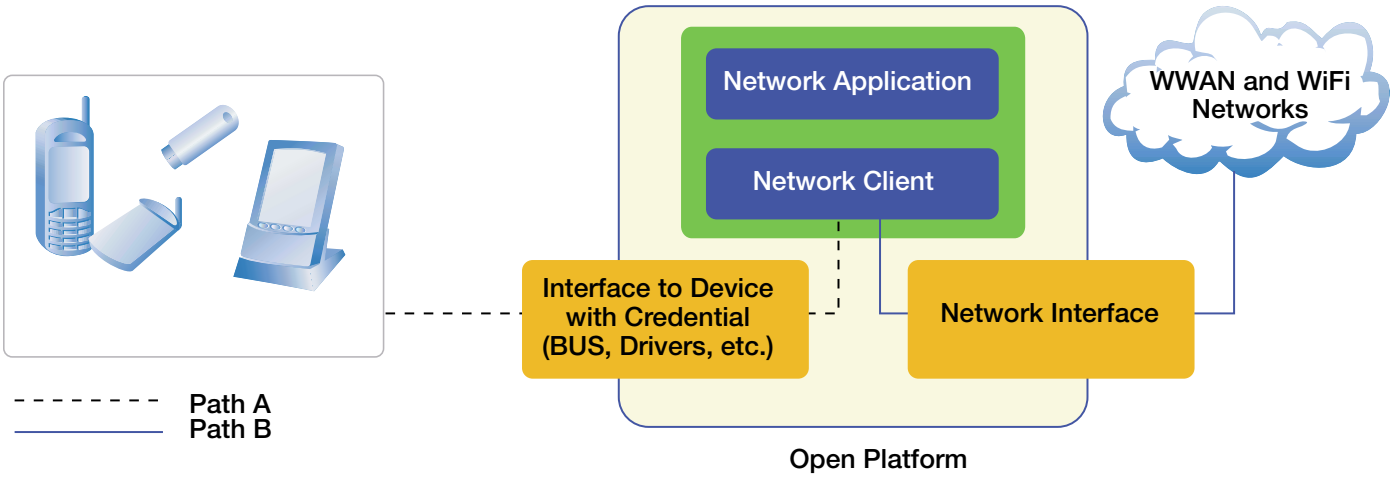

Figure 3. Open pathways

Path B is being addressed by the standards bodies with the EAP-SIM protocol and Protected Extensible Authentication Protocol (PEAP) to address data security. However, the data pathway security for Path A in open platforms has not yet been addressed in standards bodies. External SIM card readers are attached over an open bus, providing potential exposure of SIM card data. Given access to a SIM card, it is possible to obtain any number of GSM triplets and hence attack GSM security. Possible types of SIM attacks could be:

Attack on the secret key Ki: The A3A8 algorithm, Comp 128-1 is the first version of the GSM Association algorithm for internal authentication. In 1998, engineers connected with UC Berkeley were able to deduce the Ki of a SIM by collecting a large number of triplets (Rand, SRES and Kc). This type of attack is not practical if the attackers do not possess the SIM and cannot execute repeated authentication. In response to this threat, the Comp 128 was improved and will be replaced by Comp 128-2, Comp 128-3, or other proprietary algorithms. However, a large number of existing SIMs still use the old version. Therefore, it is possible for an unauthorized process running in the authentication agent of a WLAN-enabled laptop computer to perform GSM authentication commands an appropriate number of times to obtain the required triplets.

Denial of service: As a counter measure against SIM card theft and cloning, operators have implemented an authorization counter in SIM cards. This counter is incremented at every execution of the RUN GSM ALGORITHM command. This counter has a limit, generally far below the number of authentication exchanges needed to crack the algorithm, but enough to guarantee an acceptable lifetime of the SIM. Upon reaching its upper limit, the SIM becomes inoperable and needs to be replaced. So, if a hacker obtains a cloned SIM card and tries to crack the cryptographic algorithm, it is possible that the authentication counter exceeds the limit and the operator will automatically have to suspend any service associated with the SIM card. The owner of the original card will thus face denial of his or her service without being fully aware.

Spying on, or attack on the integrity of SIM data: The SIM standard states that the user pin-code (CHV1) needs to be presented before the RUN GSM ALGORITHM command can be executed. Therefore, in order to authenticate to WLAN using a standard SIM, the user will have to type in his or her CHV. This CHV gives access to most of the data in the SIM, abbreviated dialing numbers, short messages, network settings, IMSI and others. Therefore, a malicious program in the supplicant can read this data and either upload it to a cracker server or modify the contents for some criminal reasons.

Vulnerability due to these threats varies with the cryptographic algorithm used in SIM-based authentication. Comp 128-1 cryptographic algorithm is weaker than the newly defined Comp 128-3. In the future, as more operators use the Comp 128-3 algorithm, Path A security may become less of an issue.

Since the deployment of stronger forms of cryptographic algorithms is not widespread yet, PATH A security needs to be addressed. Possible ways to mitigate PATH A security issues are:

- Trusted hardware and execution environments
- Securing the data path by creating an encrypted tunnel between the SIM reader and the network client on the notebook
- An end-to-end encrypted tunnel covering Path A and Path B

Summary

Utilization of SIM for WLAN authentication could be very advantageous to operators. They can leverage existing business processes and network infrastructure. There are various ways for attaching a SIM to a notebook PC. However, accessing the SIM from a notebook PC requires consideration of some security threats.

With the appropriate mitigation approaches and in light of the advantages a SIM brings to WLAN, the industry should work on building the strength of the algorithms used in authentication and the definition of independent data structures, while enhancing the existing data that allows identification, authentication, control and service provisioning.

Feedback

Tell us what you think about this article.

More Info

Read a related article: “SIM Trust Parameters,” published in the January 2003 edition of Intel Developer Update Magazine (the previous version of this publication). Or, learn how Intel is Building the Wireless Tomorrow.

Author Bios

Ameen Ahmad is a business development/initiative manager in the Emerging Platforms Lab, part of the Corporate Technology Group. He has been at Intel for three years, and currently works on wireless technology projects in the Intel research and development group. Before Intel R&D, Ahmad was a product line manager at Intel’s Networking Software Division responsible for product strategy and marketing for wireless infrastructure software. He has worked in the telecom and high-technology industries for the last 10+ years in various product management and marketing positions. Prior to joining Intel, Ahmad was a product marketing manager for base stations at Lucent technologies. He holds an M.B.A. from the University of Chicago.

Roger Chandler is a market development manager in the Emerging Platforms Lab, part of the Corporate Technology Group. While at Intel, his areas of focus have included manufacturing process analysis, high-performance 3D technologies, and home networking. He was a 2001 recipient of an Intel Achievement Award for his work in the field of

Web 3D. Chandler is currently focused on market development strategies for Intel's many wireless technology initiatives. He holds an M.B.A. from the University of Georgia and a B.A. from the University of Tennessee.

Abhay A. Dharmadhikari is a senior software engineer in the Emerging Platforms Lab, part of the Corporate Technology Group. He has been at Intel for seven years working on a variety of projects, including adapter switching, roaming, H323-based Multi-Point Audio Server, next-generation collaboration, and location aware services. Dharmadhikari has a number of patents pending in adapter switching, networking, Multi-Point Audio Conferencing Server, indoor location detection technologies, location-based services, and security. He holds bachelor's and master's degrees in computer science from the University of Pune, India.

Uttam Sengupta is a principal engineer and the staff architect in the Emerging Platforms Lab, part of the Corporate Technology Group. In this role, he helps define EPL's long-term research agenda to complement the lab's development of advanced technology for mobile wireless client devices, including new concept platforms, system hardware and software, middleware, applications and wireless services. Prior to his current position, Sengupta worked as a software architect and director of engineering on two R&D programs, including proactive, self-healing frameworks for network management, and personalized wireless data services that proactively aggregate, prioritize, filter and deliver context-sensitive information to end users' mobile devices. Prior to joining Intel, Sengupta was an engineer at Motorola, working as a technical analyst, software architect, and software development manager for projects ranging from concurrent engineering design tools, integrated test platforms for satellite telephony and on-ground satellite cross-link testing (Iridium* LEO Telecommunication System*). He received a Ph.D. in computer science from Arizona State University and is a member of IEEE.

References

- WLAN & Bluetooth Taskforce, "Security Objectives to be included in PRD AA.39: WLAN/GSM Roaming User Scenarios," V 2.0.0, WLAN Doc 122/02.
- Mike Hendry, "*Smart Card Security and Applications*," Artech House Publishers, 2001.
- GSM Association Wireless LAN Task Force, "Advantages of using a SIM as an authentication token for Wireless LANs."
- Jane Dashevsky, Edward C. Epp, Jose Puthenkulam, and Mrudula Yalemanchi, "SIM Trust Parameters," Intel Developer Update Magazine, January 2003.
- Micehel Mouly and Marie-Bernadette Pautet, "*The GSM System for Mobile Communications*," *1992.*
- W. Rankl and W. Effing, "*SmartCard Handbook*," John Willey Publication, Second Edition, 1999.
- European Telecommunication Standards Institute, *GSM 11.11, Version 5.0*, 1995.

—End of Technology@Intel Magazine Article—